1836 (Rev. 02-01) IS, Formerly M-1200

TREASURY DOCUMENTATION

Subject
Passwords

For
SECURITY GUIDE

Also See

Identification ET-03175
Policy

Effective 7-1-2004

Replaces
ET-03113 (1-1-1997)

A password serves as a personal key to the computer systems needed for the performance of job functions. It is one authentication method of identifying a user or application before granting or denying access to Department of Treasury confidential and sensitive information. A password helps determine accountability for all transactions and other changes made to system resources including data; therefore, each user must select and manage it to protect against unauthorized discovery or usage. Applications and systems that require passwords must have the capability to generate passwords that comply with this Policy. The purpose of this Policy is to establish a standard for creation and use of strong passwords, the protection of those passwords, and the frequency of change for such passwords to prevent compromise of confidential information.

This Policy applies to all personnel who have or are responsible for an account, have access to any system/application that resides at any Treasury facility, have access to the State of Michigan network or stores any non-public Treasury information.

This Policy will reduce the risk of unauthorized access to Treasury confidential and sensitive information and network resources (i.e., network, applications, servers, databases and e-mail) by requiring:

- Users, applications and systems to be authenticated to Treasury network resources through the use of a unique password prior to allowing access.

- Passwords to be revoked after several failed login attempts.

- Pre-existing (default) and temporary passwords to be changed immediately.

- Users to use only his or her password.

- Password to be kept secret (i.e., not shared with anyone).

- The establishment of new or temporary passwords by privileged users, database administrators or system administrators, whichever is applicable.

- Strong passwords for the establishment and modification of passwords.

- Passwords to be a minimum of eight alphanumeric characters in length, a combination of upper and lower case and special characters, if the system allows.

- Passwords to be changed on a monthly basis if the application, database or system does not predetermine the frequency.

Approving Signature

- Passwords to be stored and transmitted encrypted.

- Passwords to be changed immediately if secrecy may have been compromised.

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) to be changed monthly.

- New or enhanced applications, databases or database applications to have the capability to:

  - Store and transmit passwords encrypted.
  - Enforce the use of strong passwords.
  - Generate and change its password in compliance with this Policy.

To ensure passwords that authenticate users and applications to Treasury confidential or sensitive information, the following actions are prohibited:

- Sharing passwords.
- Writing down passwords.
- Sending passwords through e-mail.
- Hard coding passwords into any program source code or workflow language.
- Storing of application and database passwords in the documents tree of a Web server.
- Use of formatted passwords.

Users of and Applications Which Access Treasury Network Resources

Each user is accountable for selecting, changing and maintaining the confidentiality of his or her passwords. Users and applications accessing Treasury confidential or sensitive information must construct and maintain each password in accordance with the following requirements:

- Select a password with a minimum of:

  - Eight alphanumeric characters in length, when the system allows. If not permissible, the minimum length is six alphanumeric characters.

  - Four distinct characters and no more than three alphabetic characters in a row.

- Create a strong password. It must contain a combination of upper and lower case alphabetic and numeric characters. The password must be a combination of two upper and lower case characters and have at least two numeric characters. (Numeric characters should not be at the beginning or the end of the password.) Special characters (!, @, #, $, %, ^, &, *, (,), +, =, /, <, >, ?, ;, :, \) should be included in the password where the computing system permits.

- Choose passwords that are not easy to decipher and are not trivial, predictable or obvious passwords.

  - Trivial passwords include common words like "secret," "password," "computer," etc.

  - Predictable passwords include days of the week, months, a new password that has only one or two characters different than the previous one, or a keyboard pattern such as "qwertyui."

  - Obvious passwords include names of persons, relatives, pets, cities, streets, own UserID or user name, an anagram of UserID, social security number, birth date, nickname, car license plate, etc.

- Avoid using dictionary words or acronyms as passwords.

- Keep each password confidential. Do not share or divulge a password to anyone.

- Do not write down a password.

- Change password routinely. Most State systems contain a password aging routine that forces users to change their password at predetermined intervals.

- Never reuse the same password when required to change a password. Most State access control systems have a minimum time period before allowing reuse of an expired password. Typically, a user may not reuse a password for 12 to 18 months.

- Never ignore a password expiration notice. Change password immediately. Most expirations are immediate, however, a maximum of six grace logons are allowed on Novell before a user is denied system access.

- Enable the password-protected screen saver every time the workstation is not in use/vacated, even if for five minutes.

- Do not use auto logon, application remembering (such as the "Remember Password" feature of applications), embedded scripts or hardcoded passwords in client software. Accepting such an offer permits anyone who has physical access to the system complete access to information technology resources.

  Exceptions may be made for specific applications (like automated backup) with the approval of the Office of Security. A procedure must exist for change of the password before approval will be granted for an exception.

- Change password immediately if it is forgotten or suspected that it is known by anyone, or its security is in doubt.

Password Assignment

Staff within each division, office or bureau have been designated as Usercode Managers to assign starter passwords and issue temporary passwords for the Global Security system (commonly referred to as MIPC and CTC-Bridge). To ensure password confidentiality, each user must change this password immediately after the first access to the system. Passwords are assigned by the following organizations for the associated systems:

System	Password Assigned By
Novell	Department of Information Technology
MAIN	Department of Management and Budget
MIPC	Usercode Manager, Department of Treasury
DCDS	Office of Security, Department of Treasury

The Office of Security, Usercode Manager, Security Administrator or applicable system HelpDesk staff must authenticate the user before issuing a temporary password.

Certain security systems such as Global Security, DCDS and MAIN will prompt the user to change his or her password at first logon. Immediately change a newly assigned password to maintain password secrecy and minimize its compromise.

Password Change Frequency

Most systems require password changes within a prescribed period. These systems send a warning prior to the expiration to permit change during a convenient period and prevent work interruption (Novell allows six grace logins prior to expiration). After the expiration of a password, the user cannot gain system access without the assistance of DIT, e-Help Desk, a usercode manager or person designated as a security administrator for a particular system.

The following common applications to which Treasury users access require predefined intervals for password change.

Application	Change Password After
Novell	90 days
MIPC/CTC-Bridge	15 logon days
STAR	15 logon days
MAIN	186 days
Treas_LAN	90 days
DCDS	45 days

All other user-level passwords (e-mail [GroupWise], Web, desktop computer, etc.) must be changed at least every month, unless otherwise required by the application.

Compromise of Password

Each user must request a temporary password when the permanent password is forgotten or if there is reason to suspect that the password was stolen or compromised. Immediately change a compromised password, notify immediate supervisor, and then notify Office of Security of the circumstances. Provide pertinent information related to the incident including the date and time password was changed, an approximate date and time of last use by user and when it was compromised on form 4000 INCIDENT REPORT. This information is extremely important in developing a time line for possible unauthorized activity.

New or Enhanced Application and Database Requirements

Applications, databases and database applications that store or access Treasury confidential or sensitive information must:

- Require the entry of a password prior to allowing access to the application.
- Authenticate individual users or groups of users.
- Contain edit compliance to enforce strong passwords.
- Immediately require change of initial passwords prior to allowing login.
- Revoke passwords after several unsuccessful login attempts.
- Store passwords using a one-way encryption method.
- Restrict setting of initial passwords to a security administrator or database administrator authorized to change passwords.
- Release or clear the memory containing a password immediately following authentication.
- Store passwords in a file separate from the executing body of the program code.
- Physically separate database passwords from other areas of code. The file containing passwords may have no other code but the passwords and any functions, routines or methods that will be used to access the password.
- Require users to change passwords monthly.
- Require several seconds after a failed login attempt before the application requests another password.
- Keep a password history and perform a check against the history to verify the password has not been previously used for a minimum of one year.

- Notify user of last successful login.

- Notify user of an unsuccessful login attempt.

- Allow for a password expiration date.

- Monitor login attempts and report failures.

- Maintain a record of when a password was changed, deleted or revoked.

New or enhanced applications, databases and database applications that store or access Treasury confidential or sensitive information must have the capability to prohibit:

- Use of common dictionary words.
- Viewing of passwords by anyone or anything except the password system.
- Reissuing a previous password by security administrators or database administrators.
- Reuse of passwords for a minimum of one year.

Use of Passwords and Pass Phrases for Remote Access Users

Remote access to the State of Michigan network is to be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase. Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all and the private key that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Password Protection

User accounts that have system-level privileges granted through group memberships or programs should have a unique password from all other accounts held by that user. Passwords should not be inserted into e-mail messages, as those records may be viewed by network administrators or possibly by hackers.

Users must not use the same password for State accounts as for other non-State access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, users should not use the same password for different State applications. The exception to this is where a Single Sign-On System may control multiple systems.

Users must not share passwords with anyone, including supervisors, administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Treasury information. Users should never write down and store passwords anywhere in their office nor should users store passwords in a file on **any** computer (including Personal Digital Assistants or similar devices).

Password Monitoring

The Office of Security or its delegates may utilize security tools to perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these audits, the user will be required to change it.

Policy Violations

An employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment, and/or lose of access rights to network resources.

End